



AIR NATIONAL GUARD (ANG) ACTIVE DUTY FOR OPERATIONAL SUPPORT (ADOS) ANNOUNCEMENT

IAW the ADOS Application Procedures

Please submit complete ADOS applications as 1 PDF to usaf.jbanafw.ngb-hr.mbx.HR-ADOS@mail.mil

If unable to encrypt or the application is over 4MB, please forward via <https://safe.amrdec.army.mil/safe/> to the above address

ANNOUNCEMENT NUMBER: 20-021 R1

CLOSE OUT DATE: 6 Sep 2020

POSITION TITLE: Comm Cyber Surety Technician

POSITION INFORMATION: Length: 30 Sep 21
Tour intent is remainder of FY20 through FY21
Pending Funding and Airman's continued eligibility.
ADOS, Title 10 - 12301d

RANK/GRADE REQUIREMENT: SSgt/E-5 to MSgt/E-7

AFSC REQUIREMENT: 3D05/7

SECURITY CLEARANCE REQ: Top Secret
(Member must have appropriate clearance for the position)
*Must have SEI: 264 Information Assurance Technical Level 2

LOCATION: ANGRC CCYC, Joint Base Andrews, MD

WHO MAY APPLY: Qualified ANG members only

POC Position:
Mr. William Funk
william.funk.8@us.af.mil
DSN: 612-7817
Comm: 240-612-7817

Position Description (Duty Description):

Supports the principles of availability, integrity, confidentiality, authentication, and non-repudiation of information and information systems for the purpose of protecting and defending the operation and management of Air Force (AF) information technology (IT) and National Security System (NSS) assets and operations. As delegated/directed by the installation/wing/unit commander, manages the overall communication security (COMSEC) posture of the organization. Serves as the COMSEC Responsible Officer (CRO) and Secure Voice Responsible Officer (SVRO). Complies with all applicable laws and regulations. Provides guidance and training to COMSEC users. Report deviations from established COMSEC and security guidelines. Assures semi-annual functional reviews are performed.

Ensures appropriate operational security posture is maintained for AF IT under their purview, maintains situational awareness, and initiates actions to improve or restore cybersecurity posture. Serves as the Computer Security (COMPUSEC) Manager. Establishes and publishes base-wide policy, as needed. Serves as Information Systems Security Manager (ISSM). Manages and provides guidance/assists in the preparations of all Risk Management Framework (RMF) packages in accordance with prescribed directives. Assists users in determining equipment requirements to prescreen and determine if proposed system meets current COMPUSEC needs of the user requirements, to include future expansion.

Uses security software and hardware tools to gather information and manage security on networks. Analyzes the information gathered and determines vulnerabilities, threats, and detection of compromises. Assists with investigating agencies in cases of sensitive matters. Ensures cybersecurity workforce is identified, trained, certified, qualified, tracked, and managed in accordance with (IAW) Department of Defense (DoD) and AF cybersecurity Workforce Improvement Program (WIP) directives and policies such as DoD Directive (DoDD) 8570.01, DoD 8570.01-M, AF manual (AFMAN) 33-210, and AFMAN 33-285. Ensures proper identification of manpower and personnel assigned to cybersecurity functions and will ensure this information is entered and maintained in the appropriate Air Force personnel databases.

Serves as the Telecommunications Monitoring and Assessment Program (TMAP) Manager. Evaluates, advises, and trains agencies organizations on TMAP requirements. Manages and serves as the Protective Distribution System (PDS) point of contact. Advises, trains, and maintains PDS requirements according to directives. Assists in the management of the Emissions Security (EMSEC) program. Prepares, documents, and manages EMSEC requests from start to final inspection. Complies with EMSEC directives and submits required reports. Conducts user education. Establishes, maintains, and exercises Information (INFOCON) adjustment plans and procedures. Responds to downward directed and local INFOCON change requirements. Manages and serves as the Protective Distribution System (PDS) point of contact. Advises, trains, and maintains PDS requirements according to directives. Provides IA guidance with respect to advice to hardware and software additions or configuration changes. Prepares and maintains required SAR forms, User agreements, Training, Inspections, and Appointment

Letters according to directives. Analyzes and provides relevant IA requirements as part of planning to ensure new systems or support to customers fall within compliance of associated directives. Performs other duties as assigned. (ADOS-274)

